ATTORNEY PROFESSIONALISM FORUM

To the Forum:

I just received a tablet device for my birthday. I not only use my tablet for personal reasons (i.e., surfing the Web, accessing my accounts on various social media websites, watching movies, as well as sending and receiving personal emails with family and friends) but I recently found that I can use my tablet for work related to my legal practice. The tablet allows me access to almost all of the same applications I use in the office (email, word processing programs, discovery and legal research software, billing systems, etc.) and I can access these applications (as well as most Internet websites and apps) through either a cellular data network or by way of accessing a wireless Internet hotspot. Most of the wireless hotspots I've accessed allow me to instantly connect to a wireless signal with the click of a few buttons. However, I am never asked to enter a password to access these various hotspots. I have recently read that cyber attacks are increasing at a disturbing rate and such activity oftentimes occurs through hacking over public wireless networks.

I want to act professionally and in a manner consistent with my ethical responsibilities to both my clients and opposing counsel. Are there certain obligations that I must abide by when using a mobile device for work-related purposes, especially with respect to accessing, transmitting and receiving confidential information through the device? How many passwords should I have on my device to make sure it is protected from unauthorized access? Am I obligated to stay informed of technological developments relating to the use of mobile devices? Last, am I required to set forth in the engagement letter with potential clients a stated protocol for the use of electronic communications in connection with a representation?

Sincerely,
Tech Geek

Dear Tech Geek:

At the risk of sounding like a couple of "techies," before we can address the issue of your professional responsibility here and the various ethical obligations associated with the use of mobile devices, it is important to have an understanding of how mobile technology is being utilized as part of current legal practice. Mobile devices and apps have become an integral part of practicing law. They allow you to be away from your physical office even when you need access to various electronic resources. In essence, mobile devices and apps allow your office to almost always be with you. Mobile devices allow us not only to have access to our work emails and voicemails but they have become convenient tools to access most if not all of the computer network applications that you would find on your office system. Examples include: document management systems, productivity applications (such as word processing, spreadsheet and presentation creation programs), discovery database programs, billing software and Internet work voicemail.

The state and federal courts in New York have embraced the use of mobile technology. Indeed, beginning in 2006, the New York State Office of Court Administration began installing free wireless Internet access in a number of New York state courthouses. As for their federal counterparts, in 2010, by Standing Order M10-468, the United States District Court for the Southern District of New York gave attorneys admitted to practice in the Southern District the opportunity to apply for a service pass which would enable them to bring one electronic device with them at a time into any of the courthouses in the district. Previously, all attorneys were required to turn over any and all electronic devices in their possession to security personnel before entering any of the courthouses in the Southern District of New York. However, the service pass program does not authorize attorneys to carry laptops into courtrooms and attorneys with service passes must request permission from individual judges to bring a laptop to court.

Another advantage of mobile technology is that it allows an attorney to conduct legal research and background searches almost instantly. Research database programs can be easily accessed in court from a mobile device either through a mobile web browser or through apps that many of the players in the research database industry have developed for use on both smartphones and tablets. Moreover, one can research prospective jurors while in court as jury selection unfolds. *See* Robert B. Gibson and Jesse D. Capell, *Researching Jurors on the Internet – Ethical Implications*, New York State Bar Association *Journal*, November/December 2012, Vol. 84, No. 9.

So where are the dangers? One of the most prevalent threats faced by those using mobile technology is the chance of physical access by unauthorized users. Almost everyone has either lost or had a device stolen. Lost or

The Attorney Professionalism Committee invites our readers to send in comments or alternate views to the responses printed below, as well as additional hypothetical fact patterns or scenarios to be considered for future columns. **Send your comments or questions to: NYSBA, One Elk Street, Albany, NY 12207, Attn: Attorney Professionalism Forum, or by e-mail to journal@nysba.org.**

This column is made possible through the efforts of the NYSBA's Committee on Attorney Professionalism. Fact patterns, names, characters and locations presented in this column are fictitious, and any resemblance to actual events or to actual persons, living or dead, is entirely coincidental. These columns are intended to stimulate thought and discussion on the subject of attorney professionalism. The views expressed are those of the authors, and not those of the Attorney Professionalism Committee or the NYSBA. They are not official opinions on ethical or professional matters, nor should they be cited as such.

stolen devices are easily susceptible to access by a third party depending on what security measures are installed on the device, even though many devices contain a PIN (personal identification number) that if not entered correctly after multiple attempts will lock the device from access for a given period of time. Another threat to mobile device users comes from unauthorized hackers who access data exchanged over unsecured wireless networks. Your mobile device is at risk for unauthorized access if no encryptions are set for either the device or the network that the device is running on. *See* Vincent J. Syracuse and Amy S. Beard, *Attorney Professionalism Forum*, New York State Bar Association *Journal*, February 2012, Vol. 84, No. 2. *See also* State Bar of Calif. Standing Comm. on Prof. Resp. and Conduct Formal Op. No. 2010-179 (2010) (discusses various factors that attorneys should consider when accessing potentially unsecured wireless networks).

Turning to your first question, there are a number of ethical obligations associated with the use of mobile devices and the duties arising with regards to preserving confidentiality. Rule 1.1 of the New York Rules of Professional Conduct (RPC) establishes our ethical obligation to provide competent representation. This includes understanding how technologies are utilized in connection with a given representation and suggests that attorneys should be intimately familiar with those technologies.

Rule 1.6 of the RPC prohibits disclosure of confidential client information without the client's informed consent. Specifically, Rule 1.6(a) of the RPC states that "[a] lawyer shall not *knowingly* reveal confidential information, as defined in this Rule, or use such information to the disadvantage of a client or for the advantage of the lawyer or a third person . . . ." (emphasis added). As defined by the RPC, confidential information "consists of information gained during or relating to the representation of a client, whatever its source, that is (a) protected by the attorney-client privilege, (b) likely to be embarrassing or detrimental to the client if disclosed, or (c) information that the client has requested be kept confidential" but "does not ordinarily include (i) a lawyer's legal knowledge or legal research or (ii) information that is generally known in the local community or in the trade, field or profession to which the information relates." *Id.* Rule 1.6(c) states that "[a] lawyer shall exercise reasonable care to prevent the lawyer's employees, associates, and others whose services are utilized by the lawyer from disclosing or using confidential information of a client, except that a lawyer may reveal the information permitted to be disclosed by paragraph (b) [of Rule 1.6] through an employee."

The Comments to Rule 1.6 also offer guidance on an attorney's duty to preserve and protect confidential information. Comment [16] to Rule 1.6 of the RPC states:

> Paragraph (c) [of Rule 1.6 of the RPC] requires a lawyer to exercise reasonable care to prevent disclosure of information related to the representation by employees, associates and others whose services are utilized in connection with the representation. *See also* Rules 1.1, 5.1 and 5.3. However, a lawyer may reveal the information permitted to be disclosed by this Rule through an employee.

Furthermore, Comment [17] to Rule 1.6 of the RPC provides:

> When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to use a means of communication or security measures not required by this Rule, or may give informed consent (as in an engagement letter or similar document) to the use of means or measures that would otherwise be prohibited by this Rule.

Both Comments [16] and [17] are highly relevant, especially in situations where an attorney supervises those handling confidential and sensitive information on his or her behalf (i.e., document service providers, information technology (IT) staff, electronic discovery consultants, as well as contract or temporary attorneys). In addition, Comment [17] provides guidance as to how an attorney should utilize mobile devices when accessing confidential information. For example, it might not be a good idea for an attorney to check work email or document servers on a mobile device when using an unsecured wireless network. The use of an unsecured wireless network creates an increased risk that confidential information viewed on the device could come into the hands of an unintended recipient by way of hacking or improperly accessing data exchanged over that particular unsecured network. Even prior to the enactment of the RPC, an opinion published by the New York State Bar Association (NYSBA) Committee on Professional Ethics found that "[l]awyers have a duty under DR 4-101 [the former Code of Professional Responsibility] to use reasonable care when transmitting documents by e-mail to prevent the disclosure of metadata containing client confidences or secrets." *See* N.Y. State Bar Op. 782 (2004).

With the constant advances in technology, we would suggest the following best practices for the use of mobile devices in your legal practice. First, if you have an IT staff at your firm, you should get to know them and make them your best friends. Or if you are

at a smaller firm, be sure to develop a close working relationship with any third-party IT vendors that may be hired to manage the firm's computer systems. Second, be competent in the areas of mobile technology usage. Last, and in direct response to your question, attorneys must keep pace with the ever-changing technological developments in mobile technology usage, and in particular, data security. *See* N.Y. State Bar Op. 842 (2010).

You should also be cautious when accessing wireless networks with a mobile device because it carries the risk of allowing others unauthorized access to confidential information. Some things to take into consideration include knowing what security measures are in place, the sensitivity of the information, how the potential dissemination of such information would affect the client, and the urgency to have access to a potentially unsecure wireless network based on the circumstances at issue, and client preference with regard to what forms of communication should be used. *See, e.g.*, State Bar of Calif. Formal Op. No. 2010-179. Very often, the potential for hacking or gaining improper access to data is far greater over a public wireless network than through the device's usual operating network (i.e., the 3G or 4G carrier network in which the device is normally operating or a secured and encrypted wireless network).

The factors set forth in the California Ethics Opinion are highly instructive for our modern and often virtual legal workplace, especially since Internet access has become so far-reaching that many airlines now allow passengers the ability to access their offices when in flight. Let's say for example that a lawyer is on a nonstop flight from New York to the Far East, and her client emails her requesting that she include, as part of a previously planned electronic court filing, a number of confidential documents under seal. Before she left for the airport, the lawyer had planned to have a colleague in her office transmit the electronic filing to the court while she was in flight since the filing deadline was to occur sometime when her plane was over the middle of the Pacific Ocean. Because of this request, however, the confidential documents in question must be emailed back and forth between the lawyer, the client and the lawyer's office during the flight. The lawyer did not have to enter any encryption passwords to access the plane's wireless network. An enterprising fellow passenger is somehow able to gain access to the lawyer's confidential communications (which include attachments consisting of the aforementioned confidential documents). Would that lawyer be protected because the urgency of the situation required her to access a potentially unsecured wireless network to meet a court deadline?

The opinion out of California suggests that, under these circumstances, accessing such a network may be permissible since a court filing deadline was imminent. That being said, absent a true emergency, why take the risk? Although many of us often act as if everything can wait until the eleventh hour, our clients deserve better. Attorneys should be forewarned not to leave such sensitive matters to the last minute, especially when their only option is to transmit confidential information over a network with little or no security. In addition, attorneys should be cautioned that unfamiliar wireless networks carry with them the risk that data exchanged on such networks could be breached.

It should be the basic rule of every law office that every mobile device used for work-related purposes contain password-protections, perhaps even utilizing multiple passwords throughout the device in question in order to access any confidential information contained therein. Confidential information may be included not only in email communications but also any documents located on a work server which can be accessed on the device. If you are at a firm and are permitted to use a personal mobile device for work purposes, make sure to follow all policies instituted by your firm as to the use of such device when handling confidential information.

Your last question asks whether you must set forth in the engagement letter with potential clients a stated protocol for the use of electronic communications in connection with a representation. We highly recommend making use of such protocol since email communications with clients have been and are an integral part of the attorney-client relationship. In our view, client engagement letters should include language disclosing the risks and confirming the client's consent to the use of electronic and mobile communications during the representation. Some sample language could include the following:

> In the course of our representation of our clients, we have a duty to preserve the confidentiality of our communications with our clients and other information relating to the representation. We need to recognize that all means of communication are, to some degree, susceptible to misdirection, delay or interception. Email and cellular telephone communications present special risks of inadvertent disclosure. However, because of the countervailing speed, efficiency, and convenience of these methods of communication, we have adopted them as part of the normal course of our operations. Unless instructed in writing to the contrary, we will assume that our clients consent to our use of email and cell phone communications in the course of our engagement.

Mobile device usage has completely altered the way we practice law and communicate with our clients. However, as with any emerging technology, one must always take all necessary precautions, especially when it comes to preventing confidential information from ending up in the hands of unintended recipients.

Sincerely,
The Forum by
Vincent J. Syracuse, Esq.,
and Matthew R. Maron, Esq.,
Tannenbaum Helpern Syracuse
& Hirschtritt LLP

CONTINUED ON PAGE 52

CONTINUED FROM PAGE 51

QUESTION FOR THE NEXT ATTORNEY PROFESSIONALISM FORUM:

I have found that accessing various forms of social media has become a highly useful tool in my practice. However, I want to know if there are limits as to how Facebook, Twitter, LinkedIn and the like can be used in connection with handling my various client matters. For example, what are the recommended methods for conducting research on adverse witnesses or potential jurors through the use of social media? What other electronic means can be utilized to conduct such research? Most important, what ethical obligations come into play when one uses social media in these contexts?

Sincerely,

I. Tweet